PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-188906
(43)Date of publication of application : 04.07.2003

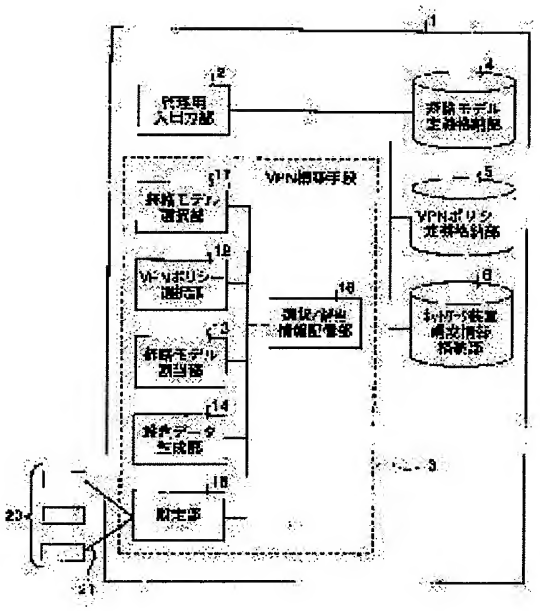
(51)Int.Cl. H04L 12/56

(21)Application number : 2001-385202
(22)Date of filing : 18.12.2001

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : SAKAMOTO YUKO
HARADA MICHIAKI
TAKANO HIROSHI
KANAEGAMI ATSUSHI

(54) VPN POLYCY MANAGEMENT DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a VPN policy management device that can easily generate set data to a plurality of devices existing on a set route in an attempt of constructing a VPN.
SOLUTION: This VPN policy management device is provided with a route model composed of a plurality of rolls expressed by functions required for constructing the VPN, a VPN policy generated correspondingly to the route model and containing another roll in part defined to each roll constituting the route model as a parameter, and configuration information containing the address information on the devices existing on the set route. This management device is also provided with a VPN constructing means 3 which assigns the rolls of the route model to the devices existing on the set route when the end roll of the route model is assigned to two end points on the set route and, at the same time, sets set data to each device by generating the set data by substituting the address information on the devices corresponding to another roll extracted from the configurational information into the VPN policy using the another roll as a parameter.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－188906
（P2003－188906A）
(43)公開日　平成15年７月４日(2003.7.4)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード*（参考）
Ｈ０４Ｌ　12/56	１００ ４００	Ｈ０４Ｌ　12/56	１００Ｃ　５Ｋ０３０ ４００Ａ

審査請求　未請求　請求項の数３　ＯＬ　（全 17 頁）

(21)出願番号　特願2001－385202(P2001－385202)

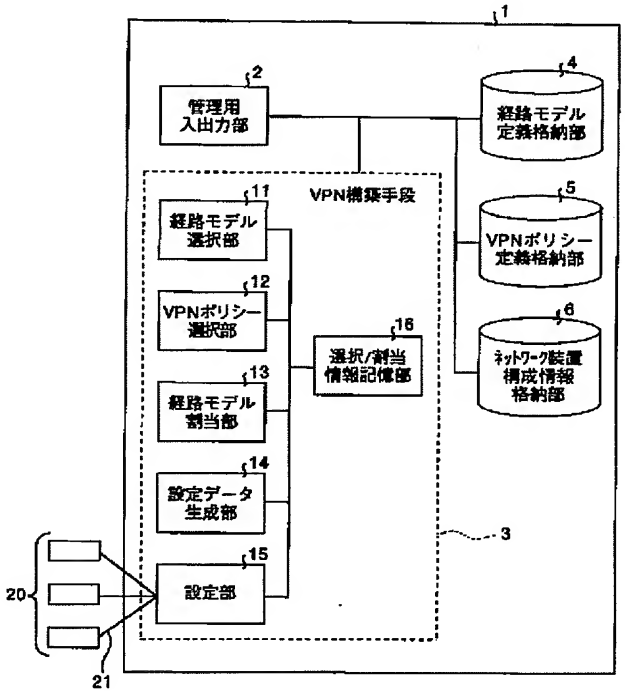
(22)出願日　平成13年12月18日(2001.12.18)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　坂本　優子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　原田　道明
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　ＶＰＮポリシー管理装置

(57)【要約】
【課題】　ＶＰＮを構築しようとしている設定経路上の複数の装置に対する設定データを容易に生成することができるＶＰＮポリシー管理装置を得ること。
【解決手段】　ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーと、前記設定経路上に存在する装置についてのアドレス情報を含む構成情報と、前記設定経路上の二つのエンドポイントに、前記経路モデルのエンドロールが割当てられると、前記経路モデルのロールを前記設定経路上の装置に割当てるとともに、他のロールをパラメータとして使用しているＶＰＮポリシーに、前記構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成し、該設定データを各装置に設定するＶＰＮ構築手段３を備える。



【特許請求の範囲】

【請求項１】　インターネットを介して接続される二つのエンドポイント間の通信経路上にＶＰＮを構築するためのＶＰＮポリシー管理装置であって、

ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルと、

前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーと、

前記設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報と、

前記設定経路上の二つのエンドポイントに、前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルのロールを前記設定経路上の装置に割当てるとともに、前記ＶＰＮポリシーの中で他のロールをパラメータとして使用しているＶＰＮポリシーに、前記構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成し、該設定データを前記設定経路上の各装置に設定するＶＰＮ構築手段と、を備えることを特徴とするＶＰＮポリシー管理装置。

【請求項２】　ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルを格納している経路モデル定義データベースと、

前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーを格納しているＶＰＮポリシー定義データベースと、

ＶＰＮを構築しようとするインターネットを介して接続される二つのエンドポイント間の設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報を有するネットワーク装置構成情報データベースと、

前記設定経路と適合する経路モデルが前記経路モデル定義データベースから選択される経路モデル選択手段と、

前記経路モデルが選択されると、該経路モデルに対応するＶＰＮポリシーが前記ＶＰＮポリシー定義データベースから選択されるＶＰＮポリシー選択手段と、

前記設定経路中に存在する装置またはセグメントをノードとし、前記エンドポイントへ向かう方向に該ノードに隣接して接続されるセグメントまたは装置を子ノードとして幅優先で配置し、同じノードが二度以上出現した場合であって、同じ経路に出現したときには該ノードは配置せずにそこでノードの展開処理を終了し、別の経路に出現したときには該ノードを配置してそこでノードの展開処理を終了し、前記設定経路中のインターネットをルートノードとしてこれらのノードを階層化して配置したツリー構造を前記構成情報に基づいて生成するツリー構造生成機能と、前記エンドポイントに対応するノードに

前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルを満たす前記ノード間の前記ツリー構造上における一以上の経路を抽出し、該一以上の経路の中から前記経路モデルを満たすノードの配置関係を有する一の経路が選択されるとともに、該経路上の装置に前記経路モデルのロールを割当てるロール割当機能と、を含む経路モデル割当手段と、

前記経路上の装置にロールが割当てられると、前記ＶＰＮポリシーの中で他のロールをパラメータとして使用しているＶＰＮポリシーに、前記ネットワーク装置構成情報データベースに格納されている構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成する設定データ生成手段と、

該生成された設定データを前記設定経路上の装置に設定する設定手段と、を備えることを特徴とするＶＰＮポリシー管理装置。

【請求項３】　前記経路モデルは、ロールごとに、該ロールが必要とする機能条件、前記設定経路上での位置が規定される構成条件、および前記ロールが前記経路モデル中で必要とされる数が定義されていることを特徴とする請求項１または２に記載のＶＰＮポリシー管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＩＰネットワーク上における端末間の通信をＶＰＮ（Virtual Private Network）で行う際に、ＶＰＮの構築および周辺装置の動作設定を簡易に行うことが可能なＶＰＮポリシー管理装置に関するものである。

【０００２】

【従来の技術】ＶＰＮ（Virtual Private Network）は、インターネットなどの信頼性の低いネットワークを介したプロジェクトメンバ間の通信において通信データを暗号化し、プロジェクトメンバ以外のユーザに対して通信を解読させないようにすることで、プロジェクトメンバだけの仮想的な専用線を提供するシステムである。図１７は、複数拠点に分散したプロジェクトメンバのために構築したＶＰＮを示す図である。図１７の５００～５０２はプロジェクトメンバが分散している距離の離れたサイトを、５１０～５１５はそれぞれのサイトに存在するプロジェクトメンバが利用するホストを、５２０～５２２はそれぞれのサイトに存在するＶＰＮ装置を、５３０～５３２はそれぞれのサイト５００～５０２に存在するＶＰＮ装置５２０～５２２間のＶＰＮをそれぞれ表わしている。サイト５００～５０２間はインターネットなどの外部ネットワークで接続されている。

【０００３】サイト５００～５０２間において、ＶＰＮ５３０～５３２を利用せずに、そのまま外部ネットワークを利用すると外部ネットワーク上の他のユーザにサイト５００～５０２間の通信データを盗聴される恐れがある。そのためサイト５００～５０２間の通信を、ＶＰＮ

装置５２０～５２２を用いて暗号化することで、ＶＰＮ（仮想専用線）５３０～５３２を提供することができる。ＶＰＮ装置５２０～５２２は各サイト５００～５０２の入り口に存在し、あるサイトのホストが他のサイトのホストと通信する際、あるホストと同じサイト上のＶＰＮ装置が通信データを暗号化した後に外部ネットワークにデータを出力し、このデータを相手サイトのＶＰＮ装置が受け取り復号化した後、発信先のホストに平文（暗号化していないデータ）のデータを送付する。このようなＶＰＮを構築するためには、図１７のＶＰＮ装置５２０～５２２間に対して暗号通信を行うためのトンネルを定義しなければならない。トンネルの定義は両端のＶＰＮ装置５２０～５２２に対して設定され、例えば、図１７のＶＰＮ装置５２０には、二つのトンネルすなわちＶＰＮ５３０、５３１に関する設定が行われる。

【０００４】また、ＶＰＮを定義するには、ＶＰＮ装置５２０～５２２の設定だけでなく通信の経路上にある図示しない複数種類の装置の設定も行わなければならない場合がある。図１８は、サイト内にファイアウォール装置を備える場合のＶＰＮの構成を模式的に示す図である。この図１８のサイト５５０において、５５１はＶＰＮ装置、５５２はファイアウォール装置である。このようにＶＰＮ装置５５１の外側にファイアウォール装置５５２が設置されている場合、該ファイアウォール装置５５２のパケットフィルタリング機能に対して暗号化されたパケットを通過させる設定を行わなければならない。またファイアウォール装置５５２がアドレス変換を行っている場合、暗号化プロトコルの種類によっては暗号化されたパケットのポート番号が変わると正しく処理できない場合があるので、暗号化されたパケットのポート番号を変更しないように設定を行う必要がある。

【０００５】図１９は、ＶＰＮ機能を持ったモバイル端末を用いて自宅等のサイト外からサイト内に接続するリモートアクセスＶＰＮの構成を模式的に示す図である。ここで、５６０はサイトを、５６１はサイト５６０のＶＰＮ装置を示している。５６２はリモートアクセスサーバであり、リモートアクセスによる接続をサイト５６０内に接続する役割を有する。そして、５６４はインターネットアクセスプロバイダのアクセスポイントを示している。

【０００６】このようなリモートアクセスＶＰＮでは、組織の建屋内からのアクセスであることが保証されているサイト間ＶＰＮと異なり、モバイル端末からアクセスしてきたユーザが本当にそのプロジェクトのメンバであるかどうかを確認するためにリモートアクセスサーバではユーザ認証と呼ばれるプロセスを実行する。このため、リモートアクセスＶＰＮでは、接続を許されたユーザのリストや各ユーザの接続先、使用可能なサービスなどについての設定も必要となる。また、リモートアクセスＶＰＮの中でも、アクセスサーバの設置方法には様々な形態があるので、通信経路上に必要とされる装置がそれらの形態によって異なるものとなる。

【０００７】このように、ＶＰＮの設定では、設定経路上に存在する複数種類の装置の設定を行わなくてはならず、またＶＰＮを構築する対象ネットワークの形態によって設定対象装置が異なる。すなわち、設定対象ネットワークの個々の装置に対してそれぞれＶＰＮの設定を行わなければならなかった。

【０００８】しかし、ＩＥＴＦ（Internet Engineering Task Force）のポリシーフレームワーキンググループが開発したＰＣＩＭ（Policy Core Information Model）およびＰＣＩＭｅ（Policy Core Information Model Extentions）では、装置に対してロール（役割）を割付け、ロールに対してポリシーを定義することを可能とした。ここで、ポリシーとは、ネットワークを構成する装置に対する設定を簡易にするための方法の一つであり、設定データを装置ベンダ固有の形式に依存しない抽象化されたデータ構造で記述するものである。これらの方法を用いることで、すべての装置に対して別々にポリシーを定義することが避けられ、ポリシー定義の作業効率が向上した。

【０００９】

【発明が解決しようとする課題】しかしながら、これらのＰＣＩＭやＰＣＩＭｅを用いた方法では、ＶＰＮ経路上の複数の装置の相互動作を考慮した上で設定を行わなければならない点は従来と同様であり、ＶＰＮ経路上の装置の設定はＶＰＮポリシー管理者の作業を煩雑にするものであるという問題点があった。

【００１０】この発明は、上記に鑑みてなされたもので、ＶＰＮを構築しようとしている設定経路上に存在する複数の装置に対するＶＰＮの設定データを容易に生成することができるＶＰＮポリシー管理装置を得ることを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するため、この発明にかかるＶＰＮポリシー管理装置は、ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーと、前記設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報と、前記設定経路上の二つのエンドポイントに、前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルのロールを前記設定経路上の装置に割当てるとともに、前記ＶＰＮポリシーの中で他のロールをパラメータとして使用しているＶＰＮポリシーに、前記構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成し、該設定データを前記設定経路上の各装

置に設定するＶＰＮ構築手段と、を備えることを特徴とする。

【００１２】この発明によれば、インターネットを介して接続される設定経路上の二つのエンドポイント間にＶＰＮを構築するためのＶＰＮポリシー管理装置が提供される。該ＶＰＮポリシー管理装置には、ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーと、前記設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報とが格納されている。そして、ＶＰＮ構築手段によって、前記設定経路上の二つのエンドポイントに、前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルのロールが前記設定経路上の装置に割当てられる。また、前記ＶＰＮポリシーの中で他のロールをパラメータとして使用しているＶＰＮポリシーに、前記構成情報から抽出された前記他のロールに対応する装置のアドレス情報が代入され、設定データが生成される。そして、該設定データが前記設定経路上の各装置に設定される。

【００１３】つぎの発明にかかるＶＰＮポリシー管理装置は、ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルを格納している経路モデル定義データベースと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーを格納しているＶＰＮポリシー定義データベースと、ＶＰＮを構築しようとするインターネットを介して接続される二つのエンドポイント間の設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報を有するネットワーク装置構成情報データベースと、前記設定経路と適合する経路モデルが前記経路モデル定義データベースから選択される経路モデル選択手段と、前記経路モデルが選択されると、該経路モデルに対応するＶＰＮポリシーが前記ＶＰＮポリシー定義データベースから選択されるＶＰＮポリシー選択手段と、前記設定経路中に存在する装置またはセグメントをノードとし、前記エンドポイントへ向かう方向に該ノードに隣接して接続されるセグメントまたは装置を子ノードとして幅優先で配置し、同じノードが二度以上出現した場合であって、同じ経路に出現したときには該ノードは配置せずにそこでノードの展開処理を終了し、別の経路に出現したときには該ノードを配置してそこでノードの展開処理を終了し、前記設定経路中のインターネットをルートノードとしてこれらのノードを階層化して配置したツリー構造を前記構成情報に基づいて生成するツリー構造生成機能と、前記エンドポイントに対応するノードに前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルを満たす前記ノード間の前記ツリー構造上における一以上の経路を抽出し、該一以上の経路の中から前記経路モデルを満たすノードの配置関係を有する一の経路が選択されるとともに、該経路上の装置に前記経路モデルのロールを割当てるロール割当機能と、を含む経路モデル割当手段と、前記経路上の装置にロールが割当てられると、前記ＶＰＮポリシーの中で他のロールをパラメータとして使用しているＶＰＮポリシーに、前記ネットワーク装置構成情報データベースに格納されている構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成する設定データ生成手段と、該生成された設定データを前記設定経路上の装置に設定する設定手段と、を備えることを特徴とする。

【００１４】この発明によれば、インターネットを介して接続される二つのエンドポイント間の通信経路上にＶＰＮを構築するためのＶＰＮポリシー管理装置が提供される。経路モデル定義データベースによって、ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルが格納される。また、ＶＰＮポリシー定義データベースによって、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーが格納される。そして、ネットワーク装置構成情報データベースによって、ＶＰＮを構築しようとするインターネットを介して接続される二つのエンドポイント間の設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報が格納される。

【００１５】まず、経路モデル選択手段のツリー構造生成手段によって、前記設定経路と適合する経路モデルが前記経路モデル定義データベースから選択される。つぎに、ＶＰＮポリシー選択手段によって、前記経路モデルが選択されると、該経路モデルに対応するＶＰＮポリシーが前記ＶＰＮポリシー定義データベースから選択される。そして、経路モデル割当手段のツリー構造生成機能によって、前記設定経路中に存在する装置またはセグメントがノードとされ、前記エンドポイントへ向かう方向に該ノードに隣接して接続されるセグメントまたは装置が子ノードとして幅優先で配置される。この際、同じノードが二度以上出現した場合であって、同じ経路に出現したときには該ノードは配置されずにそこでノードの展開処理が終了され、別の経路に出現したときには該ノードが配置されてそこでノードの展開処理が終了される。また、前記設定経路中のインターネットをルートノードとしてこれらのノードを階層化して配置したツリー構造が前記構成情報に基づいて生成される。

【００１６】また、経路モデル選択手段のロール割当機能によって、前記エンドポイントに対応するノードに前記経路モデルの終端部を定義するエンドロールが割当て

られると、前記経路モデルを満たす前記ノード間の前記ツリー構造上における一以上の経路が抽出され、該一以上の経路の中から前記経路モデルを満たすノードの配置関係を有する一の経路が選択されるとともに、該経路上の装置に前記経路モデルのロールが割当てられる。

【００１７】つぎに、設定データ生成手段によって、前記経路上の装置にロールが割当てられると、前記ＶＰＮポリシーの中で他のロールをパラメータとして使用しているＶＰＮポリシーに、前記ネットワーク装置構成情報データベースに格納されている構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データが生成される。そして、設定手段によって、該生成された設定データが前記設定経路上の装置に設定される。

【００１８】つぎの発明にかかるＶＰＮポリシー管理装置は、上記の発明において、前記経路モデルは、ロールごとに、該ロールが必要とする機能条件、前記設定経路上での位置が規定される構成条件、および前記ロールが前記経路モデル中で必要とされる数が定義されていることを特徴とする。

【００１９】この発明によれば、ロールごとに、該ロールが必要とする機能条件、前記設定経路上での位置が規定される構成条件、および前記ロールが前記経路モデル中で必要とされる数が前記経路モデルに定義される。この経路モデルによって、ＶＰＮ経路を構築するにあたって必要な装置の情報が、機能や構成で表現される。

【００２０】

【発明の実施の形態】以下に、添付図面を参照して、この発明にかかるＶＰＮポリシー管理装置の好適な実施の形態について詳細に説明する。

【００２１】実施の形態１．図１は、この発明にかかるＶＰＮポリシー管理装置の実施の形態１を示すブロック図である。ＶＰＮポリシー管理装置１は、管理用入出力部２と、ＶＰＮ構築手段３と、経路モデル定義格納部４と、ＶＰＮポリシー定義格納部５と、ネットワーク装置構成情報格納部６とを備えている。ＶＰＮ構築手段３は、さらに、経路モデル選択部１１と、ＶＰＮポリシー選択部１２と、経路モデル割当部１３と、設定データ生成部１４と、設定部１５と、選択／割当情報記憶部１６とを含む構成となっている。また、設定部１５はＶＰＮ経路上の各装置２０とネットワークなどの接続線２１を介して接続されている。

【００２２】管理用入出力部２によって、ポリシー設計者が経路モデルやＶＰＮポリシーの定義を行い、そしてＶＰＮ管理者がネットワークを構成する装置の構成情報やＶＰＮの設定を行う。経路モデル定義格納部４には、ポリシー設計者によって定義された経路モデルが格納される。ＶＰＮポリシー定義格納部５には、ポリシー設計者によって定義されたＶＰＮポリシーが格納される。ここで、ＶＰＮポリシー定義格納部５に格納されているＶＰＮポリシーは、経路モデル定義格納部４に格納されている経路モデルのいずれかと関連付けされている。また、一つの経路モデルに対するＶＰＮポリシーは複数定義することも可能である。ネットワーク装置構成情報格納部６には、ＶＰＮ管理者によって予めネットワークを構成する装置の構成情報が格納されている。ＶＰＮ構築手段３は、ＶＰＮ管理者がＶＰＮを構築するための手段であり、詳細についてはＶＰＮポリシー管理装置の動作処理手順の箇所で後述する。

【００２３】最初に、この発明で重要な役割を果たす経路モデルについて説明する。図２は、経路モデル定義格納部４に格納される定義された経路モデルの一例を示す図である。経路モデルとは、ＶＰＮの経路上に存在する設定対象装置の列を、役割（以下、ロールという）の順序列として抽象化して表現したものである。より詳しくは、設定対象となるネットワーク上の装置列を、具体的な装置名で定義するのではなく、要求される機能すなわちロールという形で順序化して表現したものである。この経路モデルは、ＶＰＮの形態別に定義される。そして、経路モデルの各ロールには、各ロールが実際の装置に割当てるために必要な適用条件が定義されている。

【００２４】例えば、図２に示される経路モデルは、サイト間ＶＰＮを定義するものであり、この経路モデルを定義する適用条件の項目として、「ロール名」、「機能条件」、「構成条件」、「最小数」および「最大数」が設定されている。

【００２５】ここで、「ロール名」は、経路モデル中でロールを一意に識別するための名称である。また、「機能条件」は、装置に各ロールを割当てる場合に装置が持つべき機能に関する条件である。

【００２６】「構成条件」は、装置に各ロールを割当てる場合に、その装置が他のロールとの位置関係において満たすべき条件である。この構成条件は、例えば一つの経路内におけるインターネットなどの信頼できないネットワークからの距離によって表現される。図２では、不等号を用いて距離の大小を表し、不等号の小さい方がよりインターネットに近いことを表している。また、この構成条件において、表中のある行はその行より上位の行で定義済みのロールとの関係で位置が決められるようになっている。ここで、構成条件の不等号にイコール（＝）が含まれている場合には、その両側のロールが同一装置に割当てられてもよいことを示している。

【００２７】「最小数」は、そのロールを割当てる装置数の最小数である。この値が０である場合には、ＶＰＮを構築するにあたりそのロールに対応する装置は必ずしも存在する必要はないことを意味している。また、「最大数」は、そのロールを割当てる装置数の最大数である。ネットワーク上では異なる目的で設置された装置であってもＶＰＮにとって同じ役割を持つ場合には、それら複数の装置に対して同じロールが割当てられる。

【００２８】つぎに、この図２に示されたサイト間ＶＰＮの経路モデルを構成する各ロールについて説明する。

【００２９】最初に、ロール名「第一エンド」、「第二エンド」について説明する。「第一エンド」、「第二エンド」というロールは通信の両端のエンドポイントを指すものである。機能条件として、「送受信機能」と定義されているが、エンドポイントに配置される装置として送受信機能を有することが必要なことを示している。エンドポイントは最優先に決められるべきロールであるため、構成条件はエンドポイントに対しては存在しない。したがって、図２中ではなんの条件も定義されていない。また、エンドポイントは必須の構成要件であるために、最小数は「１」と定義されている。最大数については、エンドポイントはグループであってもよいので、図２中では最大数が複数と設定されている。

【００３０】つぎに、ロール名「第一ＶＰＮ」、「第二ＶＰＮ」について説明する。「第一ＶＰＮ」、「第二ＶＰＮ」というロールは、ＶＰＮのトンネルの端点となるＶＰＮ装置を表わすものである。このロールに対する機能条件として、ＩＰｓｅｃ機能を有すること、そして、構成条件として、インターネットとエンドノード（エンドポイントを構成する機器）との中間に位置することが定義されている。この構成条件中で、第一ＶＰＮと第一エンドの位置関係にイコール（＝）が含まれているのは、第一エンドを割当てられたノードがＩＰｓｅｃ機能を持つ場合、このノードにさらに、第一ＶＰＮのロールを割当て、該ノードが二つのロールを有してもよいことを意味している。第二ＶＰＮと第二エンドとの関係も同様である。また、最小数、最大数ともに「１」であるので、第一ＶＰＮおよび第二ＶＰＮはそれぞれ一台必要である。

【００３１】同様に、「第一外部ファイアウォール（図中では「第一外部ＦＷ」と表記する）」、「第二外部ファイアウォール（図中では「第二外部ＦＷ」と表記する）」というロールは、機能条件として、パケットフィルタリング（ＰＦ）機能を有し、構成条件として、第一ＶＰＮまたは第二ＶＰＮよりも外側でインターネットよりも内側に位置する装置であり、この経路モデルでは無くてもよいし、複数設けてもよいことを表している。また、「第一内部ファイアウォール（図中では「第一内部ＦＷ」と表記する）」、「第二内部ファイアウォール（図中では「第二内部ＦＷ」と表記する）」というロールは、機能条件として、パケットフィルタリング（ＰＦ）機能を有し、構成条件として、第一ＶＰＮまたは第二ＶＰＮよりも内側で第一エンドポイントまたは第二エンドポイントよりも外側に位置する装置であり、この経路モデルでは無くてもよいし、複数設けてもよいことを表している。

【００３２】なお、上述した構成条件の説明において、「内側」および「外側」という表現は、各エンドポイントからインターネットへ向かう方向を「外側」と定義したときの相対的な位置関係を表している。

【００３３】上述した経路モデルの構成条件に示されたインターネットとの位置関係から、第一エンド、第一ＶＰＮ、第一外部ファイアウォールおよび第一内部ファイアウォールが一つのサイトに存在すること、第二エンド、第二ＶＰＮ、第二外部ファイアウォールおよび第二内部ファイアウォールが別の一つのサイトに存在することが表されている。

【００３４】つぎに、上述した経路モデルとともに、この発明で重要な役割を果たすＶＰＮポリシーについて説明する。図３および図４は、ＶＰＮポリシー定義格納部５に格納される定義されたＶＰＮポリシーの一例であって、図２に示された経路モデル定義に対して作成されたＶＰＮポリシー定義を示す図である。すなわち、図２の経路モデルに関連付けされて作成されたＶＰＮポリシーを示す図である。

【００３５】この図３および図４に例示されるＶＰＮポリシーは、プロジェクトにおけるプロジェクトサーバとプロジェクトに所属する端末との間のポリシーを定義した「プロジェクトサーバポリシー」である。このＶＰＮポリシーには、プロジェクトに所属する端末からプロジェクトサーバへのｔｅｌｎｅｔ（テルネット）接続を暗号化通信により行うための規則が定義されている。

【００３６】図２の経路モデルを構成するロールのうちこのＶＰＮポリシーにおいて設定対象となるロール名は、第一ＶＰＮ、第一外部ファイアウォール、第一内部ファイアウォール、第二ＶＰＮ、第二外部ファイアウォールおよび第二内部ファイアウォールである。したがって、この図３および図４に示されるＶＰＮポリシーの例ではこれらの各ロールに対するポリシーが定義されている。

【００３７】このＶＰＮポリシーの中で、「設定先ロール」には上記した設定対象となるロール名が格納される。この「設定先ロール」に対するＶＰＮポリシーとして「規則」が設けられる。ＶＰＮポリシーは、「規則」の集合として定義されるので、一つのＶＰＮポリシーに対して複数規則が存在することもある。この「規則」は、発信元、発信先、サービスなどの設定項目を含む「条件」と、アクション、対向装置、割当などの設定項目を含む「アクション」との組み合わせとして記述される。そのため、図３および図４では、「規則」は「条件」と「アクション」のさらに細かな項目からなる。ポリシー設定者がこれらを記述することによって、「「設定先ロール」が「条件」を満たす場合には「アクション」が実行される」、という形式のＶＰＮポリシーが定義される。

【００３８】つぎに、各設定先ロールに定義される規則の内容について説明する。まず、「設定先ロール」がＶＰＮの場合、「規則」の「条件」は、方向、発信元（Ｓ

ｒｃ）アドレス、発信先（Ｄｓｔ）アドレス、サービス（Ｓｅｒｖｉｃｅ）などからなる。方向は、エンドポイントからインターネットに向かう方向を外側と定義した場合の該ロールに対応する装置を通過する情報の向きを定めるものである。例えば、エンドポイントからインターネットへ向かう場合には“ｏｕｔ”、逆の場合には“ｉｎ”となる。発信元アドレスと発信先アドレスは、コンピュータやサブネット、ユーザなど、通信を自発的に送受信するエンドポイントを定める。また、サービスは、プロトコルやＴＣＰ／ＵＤＰ（Transmission Control Protocol／User Datagram Protocol）のポート番号、ＩＣＭＰ（Internet Control Message Protocol）のタイプやコードによって識別されるＩＰネットワーク上の通信アプリケーションを指定するものである。

【００３９】一方、「規則」の「アクション」は、アクション（Ａｃｔｉｏｎ）、対向装置、割当（Ｐｒｏｐｏｓａｌ）などからなる。アクションは発信元アドレス、発信先アドレス、サービスで定義される「条件」に一致したパケットを受信した装置が行うべき動作を定義するものである。対向装置は、該ロールを割当てられたＶＰＮ装置と対になるＶＰＮ装置を定めるものである。また、割当は、暗号のアルゴリズムとしてどの方法を用いるのかなどの定義を定めるものである。なお、ロール「ＶＰＮ」に定義されるアクションには、つぎの三つの種類が存在する。

（１）通過：受信したパケットをそのまま送信する。

（２）廃棄：受信したパケットを廃棄する。

（３）暗号化：受信したパケットを指定された方法で暗号化または復号（暗号を解く）した後送信する。暗号化の場合は暗号化の方法もアクションの一部として定義される。

【００４０】つぎに、「設定先ロール」がファイアウォールの場合、「規則」の「条件」は、方向、発信元アドレス、発信先アドレス、サービスからなり、これらに記述する内容はＶＰＮの場合と同様である。一方の「アクション」は、アクションのみである。このアクションは、ＶＰＮの場合と異なり、通過と廃棄の二種類となるが、これらに記述する内容はＶＰＮと同様である。

【００４１】「設定先ロール」がアドレス変換（ＮＡＴ）装置の場合、「規則」の「条件」は、方向、発信元アドレス、発信先アドレス、サービスからなり、これらに記述する内容はＶＰＮの場合と同様である。一方の「アクション」は、アクションのみである。このアクションに記述する内容は、ＶＰＮやファイアウォールの場合とは異なり、つぎのようになる。

（１）変換：受信したパケットのＩＰアドレス等を変換した後送信する。変換の場合は変換方法も定義される。

（２）無変換：受信したパケットをそのまま送信する。

【００４２】このようにして、経路モデルの各ロールに対してＶＰＮポリシーが記述される。例えば、図３における「設定先ロール」が第一ＶＰＮであるポリシーには二つの規則が規定されており、そのうちの一つの「条件」は「方向＝ｏｕｔ；Ｓｒｃ＝第一エンド；Ｄｓｔ＝第二エンド；Ｓｅｒｖｉｃｅ＝ｔｅｌｎｅｔ」であり、この条件に対する「アクション」は「Ａｃｔｉｏｎ＝暗号；対向装置＝第二ＶＰＮ；Ｐｒｏｐｏｓａｌ＝ＡＢＣ」となっている。ここで、条件の「方向＝ｏｕｔ」は第一エンドから第一ＶＰＮの外側に送信される通信を意味している。そして、「Ｓｒｃ＝第一エンド」は発信元ＩＰアドレスが第一エンドで指定される装置であることを、「Ｄｓｔ＝第二エンド」は発信先ＩＰアドレスが第二エンドで指定される装置であることを示している。また、「Ｓｅｒｖｉｃｅ＝ｔｅｌｎｅｔ」はサービスとしてｔｅｌｎｅｔ接続を使用する場合を定めている。一方、アクションの「Ａｃｔｉｏｎ＝暗号」は上記の「条件」を満たす場合の通信は暗号化することを示している。「対向装置＝第二ＶＰＮ」は暗号化された通信の送られる装置が第二ＶＰＮで定義されている装置であることを示している。そして、「Ｐｒｏｐｏｓａｌ＝ＡＢＣ」は暗号化のアルゴリズムとして“ＡＢＣ”という名称のアルゴリズムを割当てることを示している。

【００４３】すなわち、「発信元アドレスとして第一エンドを、発信先アドレスとして第二エンドを有し、ｔｅｌｎｅｔ接続して第一ＶＰＮを外側に向かって流れる情報であるならば、“ＡＢＣ”という暗号化方法によって該情報を暗号化して第二ＶＰＮまで送信する」ことを定義している。

【００４４】図３および図４中において、枠線で囲まれている表示部分が、経路モデル内のロールを用いたパラメータである。これらの経路モデルへのＶＰＮポリシーにおいては、発信元ＩＰアドレスなど具体的な装置が決まらないと入力できない値を経路モデル内のロールをパラメータとして表現できることを特徴とする。すなわち、経路モデルに対するＶＰＮポリシーは、経路モデルに含まれる各ロールに対して、経路モデルに含まれる自分および他のロールをパラメータとして用いることを許されたＶＰＮポリシー定義方法によって作成される。したがって、経路モデル中の各ロールは、それぞれ関連付けされたポリシーによって構成されている。

【００４５】つぎに、この発明にかかるＶＰＮポリシー管理装置１を用いたＶＰＮポリシー管理方法について説明する。ただし、以下に説明するＶＰＮポリシー管理方法において、ポリシー設計者によって予め経路モデル定義格納部４に経路モデルが、また、ＶＰＮポリシー定義格納部５にＶＰＮポリシーが、それぞれ既に格納されている場合を前提とする。

【００４６】また、ＶＰＮを構築したいと考えている実際のネットワーク（以下、実ネットワークという）上の設定経路として、ＶＰＮ管理者は図５に示される経路を考えているものとする。この図５において、実ネットワ

ーク１００はサイトＡとサイトＢとがインターネットを介して接続されている。サイトＡ内にサーバＡ１０１、ホストＢ１０２およびＶＰＮ装置Ｃ１０３が存在し、ＶＰＮ装置Ｃ１０３はサイトＡとインターネットとの境界に配置されている。また、サイトＢ内には、ファイアウォール装置Ｄ（図中では「ＦＷ装置Ｄ」と表記する）１０４、ＶＰＮ装置Ｅ１０５、ホストＦ１０６、ホストＧ１０７およびホストＨ１０８が存在しサイトＢとインターネットとの境界にファイアウォール装置Ｄ１０４が配置されている。なお、この発明において、セグメントとは、直結関係を含めたすべての装置間接続のことをいうものとする。

【００４７】図６は、図５に示される実ネットワーク上の装置の構成情報である。また、この図６に示される構成情報は、ネットワーク装置構成情報格納部６に格納されているデータの形態でもある。この図に示されるように、構成情報は、装置名、ＩＰアドレス、機能を含む情報である。「装置名」には、実ネットワーク上の装置名が格納されており、「ＩＰアドレス」は該装置のＩＰアドレスが、そして「機能」には該装置の有する機能が格納されている。

【００４８】ここで、図５および図６から、サイトＡでは、ＶＰＮ装置Ｃ１０３がパケットフィルタリング機能とＩＰｓｅｃ機能とを有している。また、サイトＢでは、サイトＢとインターネットとの入り口にあるファイアウォール装置Ｄ１０４がパケットフィルタリング機能を有し、それよりも内側に位置するＶＰＮ装置Ｅ１０５がＩＰｓｅｃ機能を有している。

【００４９】この図５に示される実ネットワーク１００において、サイトＡとサイトＢにまたがったプロジェクトが存在し、サイトＡのサーバＡ１０１がプロジェクトサーバで、サイトＢのホストＦ１０６およびホストＧ１０７がプロジェクトに参加する端末であり、サーバＡ１０１と、ホストＦ１０６およびホストＧ１０７からなるグループ（以下、グループＦＧという）１０９との間にＶＰＮを張る場合のＶＰＮポリシーの処理手順について説明する。

【００５０】図７は、ＶＰＮポリシー管理装置の動作処理手順を示すフローチャートである。まず、ＶＰＮ管理者は、実ネットワーク上で、ＶＰＮを構築したい端末間の経路を抽出する。ここでは、サーバＡ４０１とグループＦＧ４１０間が、ＶＰＮを構築したい端末間の経路である。ＶＰＮポリシー管理装置１の経路モデル選択部１１は、管理用入出力部２を介してＶＰＮ管理者に対して、経路モデル定義格納部４に格納されている経路モデルを表示する（ステップＳ１）。ＶＰＮ管理者は、表示された経路モデルの中から、抽出した実ネットワークの経路と合致すると思われる経路モデルを管理用入出力部２から入力する。経路モデル選択部１１は、ＶＰＮ管理者によって入力された経路モデルを経路モデル定義格納部４より選択し、選択／割当情報記憶部１６に格納する（ステップＳ２）。ここで、ＶＰＮ管理者が、図２に示される経路モデルを選択したものとする。図８は、この図２に対応する経路モデルのロール列を示す図である。

【００５１】つぎに、ＶＰＮポリシー選択部１２は、選択／割当情報記憶部１６に格納された経路モデルと関連付けされたＶＰＮポリシーをＶＰＮポリシー定義格納部５より抽出し、管理用入出力部２を介してＶＰＮ管理者に対して表示する（ステップＳ３）。ＶＰＮ管理者は、表示されたＶＰＮポリシーの中からさらに構築しようとしているＶＰＮに適当なＶＰＮポリシーを管理用入出力部２から選択する。ＶＰＮポリシー選択部１２は、ＶＰＮ管理者によって入力されたＶＰＮポリシーをＶＰＮポリシー定義格納部５より選択し、選択／割当情報記憶部１６に格納する（ステップＳ４）。ここで、ＶＰＮ管理者は、図３に示されるＶＰＮポリシーを選択したものとする。

【００５２】ＶＰＮ管理者は、管理用入出力部２から、選択した経路モデル中のエンドポイントの二つのロールを実ネットワーク上の装置に割当てる。図３に示されるＶＰＮポリシーを図５の実ネットワーク１００上に適用する場合に、図２または図８の経路モデル２００における第一エンド２１１が図５のサーバＡ１０１（プロジェクトサーバ）に、図２または図８の第二エンド２１９が図５のグループＦＧ１０９（プロジェクトに所属する端末）に対応している。したがって、ＶＰＮ管理者は、サーバＡ１０１に「第一エンド２１１」を、グループＦＧ１０９に「第二エンド２１９」を割当てる。これらの割当てられた情報は、経路モデル割当部１３によって、選択／割当情報記憶部１６に格納される（ステップＳ５）。

【００５３】つぎに、ＶＰＮ管理者は、二つのエンドポイント間の経路上に存在するロールを、実ネットワーク上の各装置に割当てる処理を行う。割当てにあたって、最小数が１すなわち必須となっているロールから順に割当を行う（ステップＳ６）。この際、ＶＰＮ管理者は、図６に示される実ネットワーク上に存在する装置の構成情報を参照しながら割当を行う。

【００５４】図２の経路モデルでは、第一ＶＰＮ２１３および第二ＶＰＮ２１７が必須のロールであるので、まず、これらの第一ＶＰＮ２１３および第二ＶＰＮ２１７について割当てを行う。図５および図６より、サイトＡ、Ｂのどちらにもｉｐｓｅｃ機能を有する装置が一つしかなく、そのいずれもが各エンドノード（エンドポイント）とインターネットの中間に位置するという構成条件を満たすので、経路モデル割当部１３は、サイトＡのＶＰＮ装置Ｃ１０３にロール「第一ＶＰＮ２１３」を、サイトＢのＶＰＮ装置Ｅ１０５にロール「第二ＶＰＮ２１７」を割当てる。そして、割当てられた結果は、選択／割当情報記憶部１６に格納される。

【００５５】その後、最小数が０であるロールを順に割当て、その結果を選択／割当情報記憶部１６に格納する（ステップＳ７）。図５および図６より、サイトＢ間のファイアウォール装置Ｄ１０４はパケットフィルタリング機能を有し、第二ＶＰＮ２１７に対応するＶＰＮ装置Ｅ１０５とインターネットとの中間に位置しているので、ロール「第二外部ファイアウォール２１６」の適用条件を満たしている。したがって、経路モデル割当部１３は、ＶＰＮ管理者からの指示により、ファイアウォール装置Ｄ１０４にロール「第二外部ファイアウォール２１６」を割当てる。

【００５６】一方、図２または図８の経路モデル２００中の「第一外部ファイアウォール２１４」というロールは、パケットフィルタリング機能を有し、第一エンド２１１よりもインターネットの側に位置する条件を有するものであるが、図５および図６より、実ネットワーク１００上にはこれに対応する装置が存在しない。また、最小数が“０”であるので、この「第一外部ファイアウォール２１４」というロールは必須ではない。したがって、図２のロール「第一外部ファイアウォール２１４」は、図５の実ネットワーク１００上の装置には割当てられない。同様にして、図２または図８に示される経路モデル２００中の他のロール「第一内部ファイアウォール２１２」および「第二内部ファイアウォール２１８」を満たす装置も、図５の実ネットワーク１００上の装置には存在しないので、これらのロールは割当てられない。このように、すべてのロールについて割当てを行った後に、経路モデル割当部１３によるロールの割当作業は終了する。

【００５７】図９は、経路モデル割当部１３によって割当てられた実ネットワーク１００上の装置と経路モデル２００のロールとの対応関係を示す図である。図９中の点線３０１～３０５が、実ネットワーク１００内の装置と割当てたロールとの対応関係を示している。上述したように経路モデル２００への割当ての結果、サーバＡ１０１に第一エンド２１１のロールが、グループＦＧ１０９に第二エンド２１９のロールが、ＶＰＮ装置Ｃ１０３に第一ＶＰＮ２１３のロールが、ＶＰＮ装置Ｅ１０５に第二ＶＰＮ２１７のロールが、そしてファイアウォール装置Ｄ１０４に第二外部ファイアウォール２１６のロールが、それぞれ割当てられることになる。そして、これらの割当て結果は、上述したように選択／割当情報記憶部１６に格納されている。

【００５８】つぎに、設定データ生成部１４は、これらの割当結果と、ネットワーク装置構成情報格納部６に格納されている装置の構成情報と、ＶＰＮポリシーとを用いて、割当てられたこれらの個々の装置に対して設定データを生成する（ステップＳ８）。すなわち、これらの割当てられた装置のそれぞれに対して、図３に示されるＶＰＮポリシーが適用されるように設定される。ここで、設定データ生成部１４は、ＶＰＮポリシーに含まれるロールの部分に、割当結果である実ネットワーク１００上の装置の構成情報を代入する処理を行う。具体的には、ＶＰＮポリシーに含まれるロールの部分に、実ネットワーク１００上の装置の構成情報に含まれるＩＰアドレスが代入される。なお、ネットワーク装置構成情報格納部６が無い場合やネットワーク装置構成情報格納部６に該当する構成情報が入力されていない場合には、ここで管理用入出力部２よりそれぞれの装置の構成情報を入力してもよい。このようにして、各装置に適用されるＶＰＮポリシーが生成される。

【００５９】図１０は、この処理の結果として生成された設定データを表す図である。この図は、図３に示されるＶＰＮポリシーのパラメータとしてロール名が入力されている部分に、実ネットワーク上のＩＰアドレスが入力され、不要の装置についてのロールを削除したものである。そして、この設定データは、設定データ生成部１４によって選択／割当情報記憶部１６に格納される。

【００６０】その後、設定部１５は、選択／割当情報記憶部１６に格納された設定データにしたがって、実ネットワーク上の各装置に対して設定を行う（ステップＳ９）。設定部１５は、ネットワークなどの接続線２１を介して実ネットワーク上の各装置と接続されており、設定情報を各装置に送信し、設定することができる。そして、ＶＰＮを構築しようとする実ネットワーク上の装置に対するＶＰＮポリシーの設定が終了する。

【００６１】以上説明したように、この実施の形態１によれば、装置の備えるべき機能で表現されたロール列からなる経路モデルと、該経路モデルを構成する各ロールに対して定義されたＶＰＮポリシーに基づいて、設定経路にＶＰＮポリシーを設定するようにしたので、設定経路上の装置にＶＰＮポリシーを割当てるだけで、各装置に対する設定データを生成することができる。また、ＶＰＮポリシーには、各装置間の関係が関連付けされているので、ＶＰＮの構築を容易にすることができる。そして、それまで装置ごとに行っていた設定作業を、一つの経路を単位として行う設定作業とすることができ、ＶＰＮ構築の作業時におけるＶＰＮ管理者の作業負担を軽減することができるという効果を奏する。

【００６２】実施の形態２．図１１は、この発明にかかるＶＰＮポリシー管理装置の実施の形態２を示すブロック図である。この図１１において、実施の形態１と異なる箇所は、ネットワーク装置構成情報格納部６に、実ネットワーク上の装置の配置構成を示す情報についても格納される点、および経路モデル割当部１３がツリー構造生成機能１３ａとロール割当機能１３ｂとを有するように構成されている点である。その他の構成要素であって上述した実施の形態１と同一の構成要素には、同一の符号を付してその説明を省略している。

【００６３】ネットワーク装置構成情報格納部６には、

ＶＰＮを構築しようとしている実ネットワーク上の設定経路における他の装置との配置関係がさらに格納される。図１２は、ネットワーク装置構成情報格納部６に格納される設定経路上の各装置の構成情報およびセグメント情報の一例を示す図である。また、図１３は図１２に格納されている各装置の構成情報およびセグメント情報の基となるＶＰＮを構築しようとしている設定経路の模式図を示すものである。

【００６４】図１２（Ａ）に示される設定経路上の装置の構成情報は、図６に示される構成情報に加えて、各装置間の配置位置が規定される項目としての「保有インタフェース」が設けられている。この保有インタフェースには、隣接する装置との間のインタフェース名が格納される。また、図１２（Ｂ）は、ネットワーク装置構成情報格納部６に上述した（Ａ）の構成情報とは別に格納されるセグメント情報の一例を示す図である。このセグメント情報には、各装置間を接続する「セグメント名」とその「接続インタフェース」が格納される。ここで、図１３に示されるように各装置とインターネット側のセグメントとのインタフェースは、各装置の英数字に「１」を付して表し、それとは反対側の各装置とセグメントとのインタフェースは、各装置の英数字に「２」を付して表している。例えば、図１３において、ＶＰＮ装置Ｃ４０３は、インタフェースＣ１とＣ２の二つのインタフェースを有し、そのうちインタフェースＣ１はインターネット側のセグメント１と接続され、インタフェースＣ２はエンドポイント側のセグメント２と接続される。

【００６５】また、ツリー構造生成機能１３ａは、ネットワーク装置構成情報格納部６に格納されている設定経路上の装置からツリーを生成する機能を有し、ロール割当機能１３ｂは、ツリー構造生成機能１３ａによって生成されたツリーから経路モデルに適合するエンドポイント間の経路を選択し、該経路上の装置にロールを割当てる機能を有する。

【００６６】つぎに、ＶＰＮポリシー管理装置１によって、エンドポイント間の装置を自動検出する動作処理手順について図１４を参照しながら説明する。図１５は、図１３に示される設定経路を有する装置同士の隣接関係をツリー表示した図である。なお、この実施の形態２での経路モデルおよびＶＰＮポリシーは上述した実施の形態１で使用した図２および図３を用いるものとする。

【００６７】まず、ＶＰＮ管理者によって、管理用入力部２から図１３に示されるサーバＡおよびホストＦ４０７とホストＧ４０８からなるグループＦＧ４１０との間に、ＶＰＮを構築しようとしている設定経路が設定される（ステップＳ１１）。この設定においては、ＶＰＮ管理者は、ネットワーク装置構成情報格納部６より設定経路上に存在する装置を選択し、さらに該装置の配置情報を管理用入力部２より入力する。ここで入力される配置情報は、図１２（Ａ）の構成情報中の「保有インタフェース」および（Ｂ）のセグメント情報である。

【００６８】つぎに、実施の形態１の図７で説明したステップＳ１～Ｓ５と同じ処理を行って、設定経路上の装置に経路モデル上のエンドロールを割当てる（ステップＳ１２～Ｓ１６）。すなわち、経路モデルと該経路モデルに対応するＶＰＮポリシーを選択した後に、設定経路上のサーバＡ４０１に図２に例示される経路モデルの第一エンドを、グループＦＧ４１０に同じく第二エンドを割当て、選択／割当情報記憶部１６に格納する。

【００６９】その後、経路モデル割当部１３のツリー構造生成機能１３ａによって、ステップＳ１１で入力された設定経路から図１５に示されるツリー構造が生成される（ステップＳ１７）。ここで、このツリー構造を生成するための動作処理手順を図１６に示すフローチャートを参照しながら説明する。

【００７０】まず、経路モデル割当部１３のツリー構造生成機能１３ａは、ＶＰＮ管理者によって入力された設定経路から、インターネットなどの信頼性の低いネットワークをルートとして設定する（ステップＳ２１）。そして、設定したルートを最初の処理中のノードとし（ステップＳ２２）、該処理中のノードからエンドポイント方向に隣接して接続される装置またはセグメントを該ノードの子ノードとして、幅優先で配置する（ステップＳ２３）。

【００７１】ツリー構造生成機能１３ａは、子ノードとして配置されたノードを、つぎに処理中のノードとして設定する（ステップＳ２４）。そして、該処理中のノードに子ノードに対応する装置またはセグメントが存在するか否かを判断する（ステップＳ２５）。ここで、子ノードに対応する装置またはセグメントとは、処理中のノードにエンドポイント方向に隣接して接続される装置またはセグメントのことをいう。もし、処理中のノードに子ノードに対応する装置またはセグメントが存在しないと判断された場合（ステップＳ２５でＮｏの場合）には、その経路でのツリーの展開処理は該ノードで終了する。これに対して、もし、処理中のノードに子ノードに対応する装置またはセグメントが存在する場合（ステップＳ２５でＹｅｓの場合）には、該子ノードに対応する装置またはセグメントが、ツリー全体で既に存在しているか否かを判断する（ステップＳ２６）。子ノードに対応する装置またはセグメントが、ツリー全体で存在していないと判断された場合（ステップＳ２６でＮｏの場合）には、該装置またはセグメントを処理中のノードの子ノードとして配置する（ステップＳ２７）。その後、ステップＳ２４に戻って、ツリー構造生成機能１３ａによって、上述した工程が繰り返し実行される。

【００７２】一方、ステップＳ２６において、子ノードに対応する装置またはセグメントが、ツリー全体で既に存在していると判断された場合（ステップＳ２６でＹｅｓの場合）には、既に存在しているその装置またはセグ

メントに対応するノードが、処理中のノードが展開している経路中に存在するのか否かについて判断を行う（ステップＳ２８）。もし、既に存在している装置またはセグメントに対応するノードが現在展開している経路中に存在するのであれば（ステップＳ２８でＹｅｓの場合）、子ノードに対応する装置またはセグメントの配置処理は行われず（ステップＳ２９）、その経路でのツリーの展開処理が終了する。これに対して、もし、既に存在しているノードが現在展開している経路中に存在していないのであれば（ステップＳ２８でＮｏの場合）、子ノードに対応する装置またはセグメントを処理中のノードの子ノードとして配置する処理を行い（ステップＳ３０）、その経路でのツリーの展開処理は該配置したノードで終了する。このようにして全ての経路の展開が中止すると、すべての処理は終了する。

【００７３】このようにツリー構造生成機能１３ａによって、図１５に示されるツリーが図１３に示される設定経路から生成される。そして、生成されたツリーにおいて、任意の二つのノード間の経路は、実際のネットワーク上での経路と一致するものとなる。

【００７４】再び図１４に戻り、経路モデル割当部１３のロール割当機能１３ｂは、ツリー構造生成機能１３ａによって生成されたツリー上のノードに経路モデルのロールを割当てる処理を行う（ステップＳ１８）。

【００７５】ロール割当機能１３ｂは、ＶＰＮ管理者によって設定されたエンドポイント間の経路を、図１５に示されるツリーから求める。この例の場合には、つぎの二つの場合が存在することがわかる。経路（Ａ）サーバＡ４０１－セグメント２－ＶＰＮ装置Ｃ４０３－セグメント１－インターネット４１１－セグメント３－ルータＩ４０４－セグメント４－ファイアウォール装置Ｄ４０５－セグメント５－グループＦＧ４１０経路（Ｂ）サーバＡ４０１－セグメント２－ＶＰＮ装置Ｃ４０３－セグメント１－インターネット４１１－セグメント３－ルータＩ４０４－セグメント４－ＶＰＮ装置Ｅ４０６－セグメント５－グループＦＧ４１０

【００７６】つぎに、ロール割当機能１３ｂは、割当ての必須なロールである第一ＶＰＮおよび第二ＶＰＮの割当てを行う。第一ＶＰＮおよび第二ＶＰＮにはＩＰｓｅｃ機能が必要であり、またそれはインターネットと第一エンドまたは第二エンドとの中間に配置される必要がある。しかし、上記（Ａ）の経路には、ＩＰｓｅｃ機能を有する第二ＶＰＮに該当する装置が存在しないことがわかる。これに対して、（Ｂ）の経路では、ＶＰＮ装置Ｃ４０３に第一ＶＰＮを、ＶＰＮ装置Ｅ４０６に第二ＶＰＮをそれぞれ割当てることができる。したがって、ロール割当機能１３ｂは、第一エンドと第二エンドとの間を結ぶ経路として、（Ｂ）の経路を選択する。

【００７７】そして、ロール割当機能１３ｂは、選択された（Ｂ）の経路のうち、図２に示される経路モデル中の他のロールの機能および構成条件、具体的には、最小数が“０”であるロールの機能および構成条件を満たす装置を求める。この図１３および図１５に示される例では、最小数が“０”のロールとして、第一外部ファイアウォール、第二外部ファイアウォール、第一内部ファイアウォールおよび第二内部ファイアウォールがあるが、これらのロールの機能条件と構成条件の両者を満足する装置は（Ｂ）の経路上には存在しない。したがって、ロール割当機能１３ｂは、これらの最小数が“０”であるロールを割当てる装置が存在しないと判断し、これらの割当処理を行わない。これらの割当結果は、選択／割当情報記憶部１６に格納される。このようにしてすべてのロールに対して割当処理が行われた後に、設定経路上の装置の検出が終了する。

【００７８】その後、設定データ生成部１４は、これらの割当結果と、ネットワーク装置構成情報格納部６に格納されている構成情報と、ＶＰＮポリシーとを用いて、これらの個々の装置に対して設定データを生成し、選択／割当情報記憶部１６に格納する（ステップＳ１９）。そして、設定部１５は、選択／割当情報記憶部１６に格納された設定データにしたがって、接続線２１を介して接続された設定経路上の各装置に対して設定を行う（ステップＳ２０）。そして、ＶＰＮを構築しようとする実ネットワーク上の装置に対するＶＰＮポリシーの設定が終了する。

【００７９】以上説明したように、この実施の形態２によれば、インターネットをルートとした隣接関係のツリーを生成し、ツリーのエンドノードに経路モデルのエンドロールを割当てることによって、エンドノード間の経路を自動的に求めることが可能となる。そして、この方法によって、ＶＰＮ管理者は、ＶＰＮを張りたいエンドポイントを指定することにより、エンドポイント間に存在する装置構成を意識することなくＶＰＮを構築できるようになり、ＶＰＮ管理の作業効率がさらに向上する。

【００８０】

【発明の効果】以上説明したように、この発明によれば、ＶＰＮを構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むＶＰＮポリシーとを備え、設定経路上の二つのエンドポイントに経路モデルの終端部を定義するエンドロールが割当てられると、経路モデルのロールを設定経路上の装置に割当てて、ＶＰＮポリシーから設定データを生成するＶＰＮ構築手段とを備えるように構成したので、ＶＰＮを構築する設定経路上の各装置間の関係が関連付けされ、ＶＰＮの構築を容易にすることができる。また、ＶＰＮの構築にあたって、設定作業を装置ごとではなく、一つの経路を単位として行うことができ、ＶＰＮ管理者の作業負担を軽減することができるという効果を奏す

る。

【００８１】つぎの発明によれば、設定経路中に存在する装置またはセグメントの接続関係を、インターネットをノードとしたツリー構造を生成し、該ツリー構造を用いて設定経路上の装置に経路モデルのロールを割当てるように構成したので、ＶＰＮ管理者は、ＶＰＮを張りたいエンドポイントを指定するだけで、エンドポイント間に存在する装置構成を意識することなくＶＰＮを構築できるようになり、ＶＰＮ管理の作業効率がさらに向上するという効果を奏する。

【００８２】つぎの発明によれば、経路モデルが、必要とする機能条件、前記設定経路上での位置が規定される構成条件、および経路モデル中で必要とされる数によって定義された、複数のロールによって構成されているので、装置に依存しない汎用性の高い設定条件を提供することができるという効果を奏する。また、同じような構成のＶＰＮを構築する際において、経路モデルを備えることにより、ＶＰＮを構築するたびに装置の動作処理条件を設定しなくてすむので、ＶＰＮ管理者の作業効率を向上させることができるという効果も奏する。

【図面の簡単な説明】

【図１】　この発明の実施の形態１のＶＰＮポリシー管理装置の構成を示すブロック図である。

【図２】　経路モデルの一例を示す図である。

【図３】　図２の経路モデルに対応するＶＰＮポリシーの一例を示す図である（その１）。

【図４】　図２の経路モデルに対応するＶＰＮポリシーの一例を示す図である（その２）。

【図５】　ＶＰＮを構築しようとしている実際のネットワーク上の経路の一例を示す図である。

【図６】　図５の実際のネットワーク上の経路を構成する装置の構成情報の一例を示す図である。

【図７】　ＶＰＮ構築の処理手順を示すフローチャート＊である。

【図８】　図２の経路モデルのロール名を構成条件にしたがって配列した図である。

【図９】　図５の実際のネットワーク上の経路と、図８の経路モデルとの対応関係を示す図である。

【図１０】　ＶＰＮ構築手段によって生成された設定データの一例を示す図である。

【図１１】　この発明の実施の形態２のＶＰＮポリシー管理装置の構成を示すブロック図である。

【図１２】　ネットワーク装置構成情報格納部に格納されている装置の構成情報の一例を示す図であり、（Ａ）は装置の構成情報を、（Ｂ）はセグメント情報を示している。

【図１３】　この発明の実施の形態２を説明するための実際のネットワーク上の経路の一例を示す図である。

【図１４】　ＶＰＮ構築の処理手順を示すフローチャートである。

【図１５】　実施の形態２の方法によって、図１３のネットワーク構成をツリー表示した図である。

【図１６】　設定経路からツリー構造を生成する処理手順を示すフローチャートである。

【図１７】　従来のＶＰＮの構成を示す図である。

【図１８】　従来のＶＰＮの構成を示す図である。

【図１９】　従来のＶＰＮの構成を示す図である。

【符号の説明】

１　ＶＰＮポリシー管理装置、２　管理用入出力部、３　ＶＰＮ構築手段、４経路モデル定義格納部、５　ＶＰＮポリシー定義格納部、６　ネットワーク装置構成情報格納部、１１　経路モデル選択部、１２　ＶＰＮポリシー選択部、１３　経路モデル割当部、１３ａ　ツリー構造生成機能、１３ｂ　ロール割当機能、１４　設定データ生成部、１５　設定部、１６　選択／割当情報記憶部、２０装置、２１　接続線。

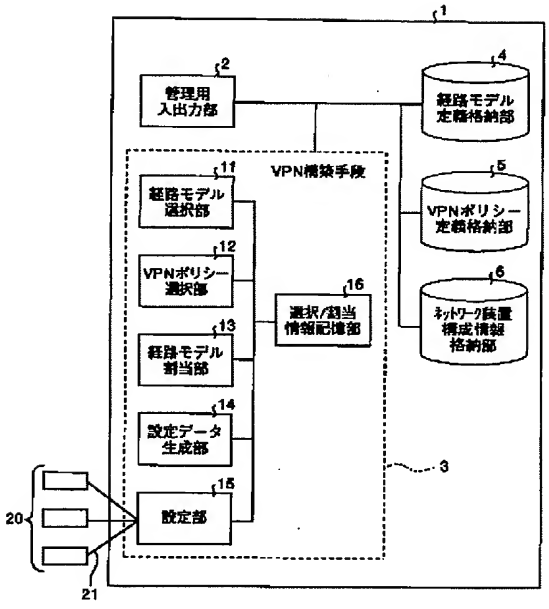
【図２】

経路モデル名：サイト間VPN経路モデル

ロール名	機能条件	構成条件	最小数	最大数
第一エンド	送受信機能	—	1	複数
第二エンド	送受信機能	—	1	複数
第一VPN	IPsec機能	インターネット＜第一VPN≦第一エンド	1	1
第二VPN	IPsec機能	インターネット＜第二VPN≦第二エンド	1	1
第一外部FW	PF機能	インターネット＜第一外部FW＜第一VPN	0	複数
第二外部FW	PF機能	インターネット＜第二外部FW＜第二VPN	0	複数
第一内部FW	PF機能	第一VPN＜第一内部FW＜第一エンド	0	複数
第二内部FW	PF機能	第二VPN＜第二内部FW＜第二エンド	0	複数

FW：ファイアウォール
PF ：パケットフィルタリング

【図１】



【図３】

VPNポリシー名：プロジェクトサーバポリシー
VPNポリシー

設定先ロール	規則	
	条件	アクション
第一VPN	方向=out Src=第一エンド Dst=第二エンド Service=telnet	Action=暗号 対向装置=第二VPN Proposal=ABC
	方向=in Src=第二エンド Dst=第一エンド Service=telnet（開始）	Action=暗号 対向装置=第二VPN Proposal=ABC
第一外部FW	方向=out Src=第一VPN Dst=第二VPN Service=IKE	Action=通過
	方向=out Src=第一VPN Dst=第二VPN Service=IPsec	Action=通過
	方向=in Src=第二VPN Dst=第一VPN Service=IKE	Action=通過
	方向=in Src=第二VPN Dst=第一VPN Service=IPsec	Action=通過
第一内部FW	方向=out Src=第一エンド Dst=第二エンド Service=telnet	Action=通過
	方向=in Src=第二エンド Dst=第一エンド Service=telnet（開始）	Action=通過

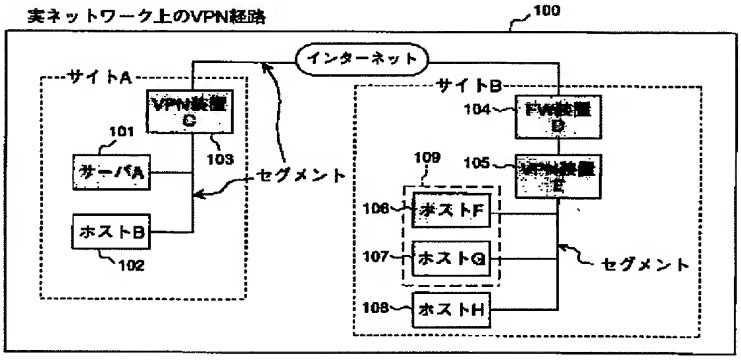
FW：ファイアウォール　Src：発信元　Dst：発信先

【図４】

設定先ロール	規則	
	条件	アクション
第二VPN	方向=out Src=第二エンド Dst=第一エンド Service=telnet（開始）	Action=暗号 対向装置=第一VPN Proposal=ABC
	方向=in Src=第一エンド Dst=第二エンド Service=telnet	Action=暗号 対向装置=第一VPN Proposal=ABC
第二外部FW	方向=out Src=第二VPN Dst=第一VPN Service=IKE	Action=通過
	方向=out Src=第二VPN Dst=第一VPN Service=IPsec	Action=通過
	方向=in Src=第一VPN Dst=第二VPN Service=IKE	Action=通過
	方向=in Src=第一VPN Dst=第二VPN Service=IPsec	Action=通過
第二内部FW	方向=out Src=第二エンド Dst=第一エンド Service=telnet（開始）	Action=通過
	方向=in Src=第一エンド Dst=第二エンド Service=telnet	Action=通過

FW：ファイアウォール　Src：発信元　Dst：発信先

【図５】

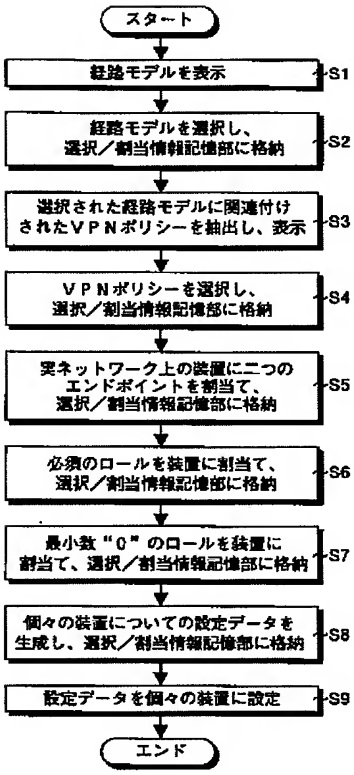


【図６】

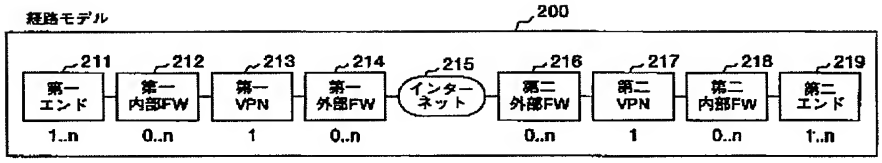
装置名	IPアドレス	機能
サーバA	133.141.10.2	送信機能、受信機能
ホストB	133.141.10.3	送信機能、受信機能
VPN装置C	133.141.10.1	パケットフィルタリング機能 IPsec機能
FW装置D	200.74.1.1	パケットフィルタリング機能
VPN装置E	200.74.8.1	IPsec機能
ホストF	200.74.8.101	送信機能、受信機能
ホストG	200.74.8.102	送信機能、受信機能
ホストH	200.74.8.103	送信機能、受信機能

FW：ファイアウォール

【図７】



【図８】

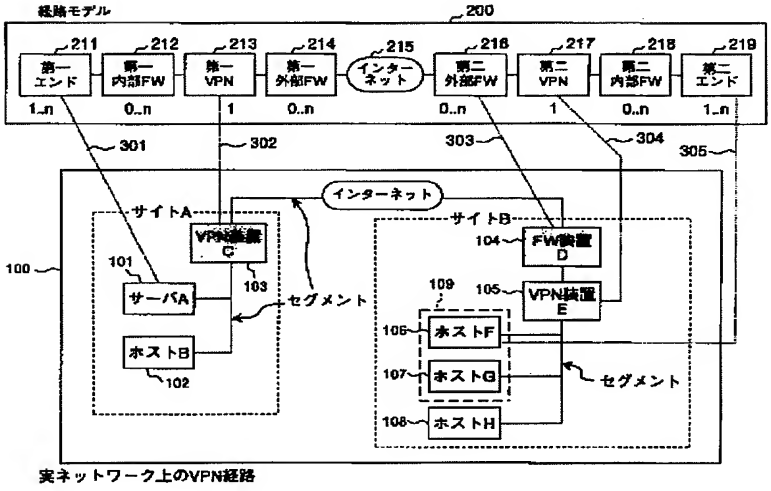


【図１０】

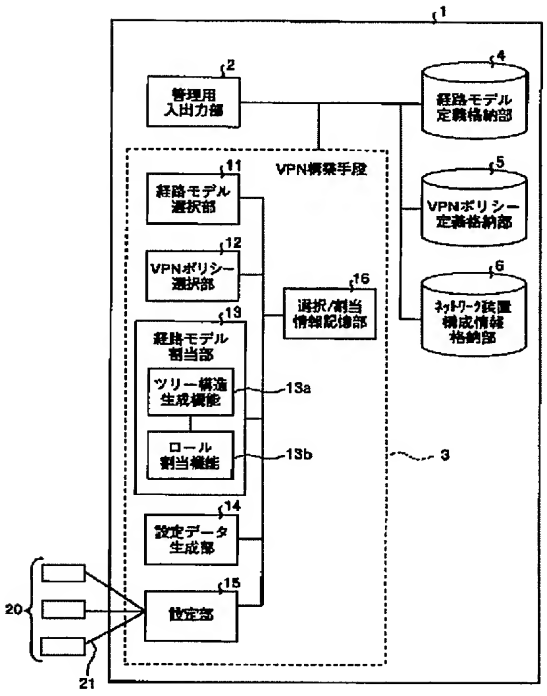
設定先ロール	規則	
	条件	アクション
第一VPN	方向=out Srcアドレス=133.141.10.2 Dstアドレス=200.74.8.101～200.74.8.102 Service=telnet	Action=暗号 対向装置=200.74.8.1 Proposal=ABC
	方向=in Src=200.74.8.101～200.74.8.102 Dst=133.141.10.2 Service=telnet（開始）	Action=暗号 対向装置=200.74.8.1 Proposal=ABC
第二VPN	方向=out Src=200.74.8.101～200.74.8.102 Dst=133.141.10.2 Service=telnet	Action=暗号 対向装置=133.141.10.1 Proposal=ABC
	方向=in Src=133.141.10.2 Dst=200.74.8.101～200.74.8.102 Service=telnet	Action=暗号 対向装置=133.141.10.1 Proposal=ABC
第二外部FW	方向=out Src=200.74.8.1 Dst=133.141.10.1 Service=IKE	Action=通過
	方向=out Src=200.74.8.1 Dst=133.141.10.1 Service=ESP	Action=通過
	方向=in Src=133.141.10.1 Dst=200.74.8.1 Service=IKE	Action=通過
	方向=in Src=133.141.10.1 Dst=200.74.8.1 Service=ESP	Action=通過

FW：ファイアウォール　Src：発信元　Dst：発信先

【図９】



【図１１】



【図１２】

装置構成情報

装置名	IPアドレス	機能	保有インタフェース
サーバA	133.141.10.2	送信機能、受信機能	C1,C2
ホストB	133.141.10.3	送信機能、受信機能	A1
VPN装置C	133.141.10.1	パケットフィルタリング機能 IPsec機能	I1, I2, I3
ルータI	200.74.1.0	ルーティング機能	B1
FW装置D	200.74.1.1	パケットフィルタリング機能	D1,D2
VPN装置E	200.74.8.1	IPsec機能	E1,E2
ホストF	200.74.8.101	送信機能、受信機能	F1
ホストG	200.74.8.102	送信機能、受信機能	G1
ホストH	200.74.8.103	送信機能、受信機能	H1

FW：ファイアウォール

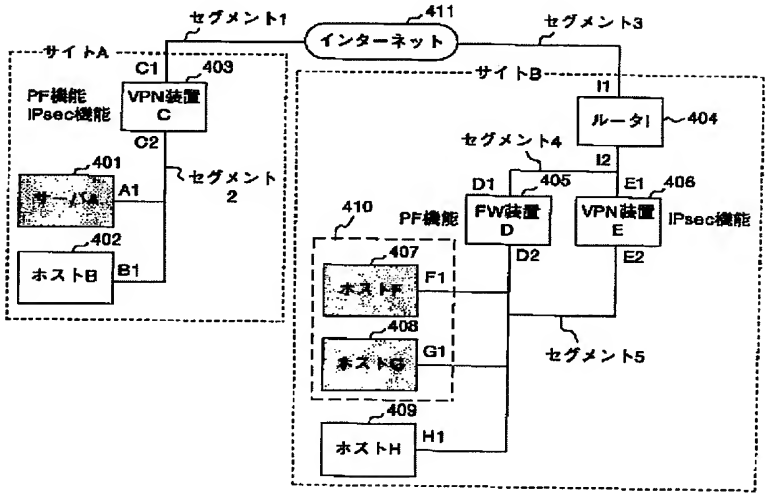
(A)

セグメント情報

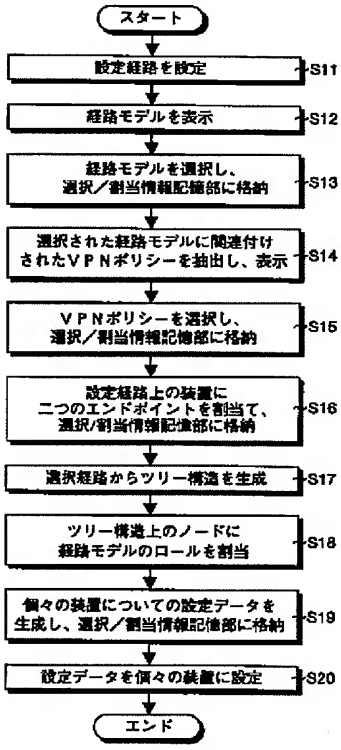
セグメント名	接続インタフェース
セグメント1	C1,（インターネット）
セグメント2	C2, A1, B1
セグメント3	I1,（インターネット）
セグメント4	I2, D1, E1
セグメント5	D2, E2, F1, G1, H1

(B)

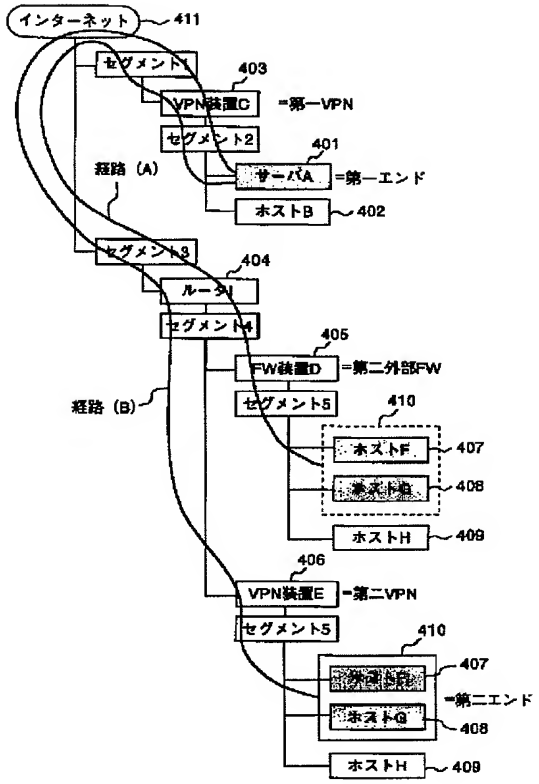
【図１３】



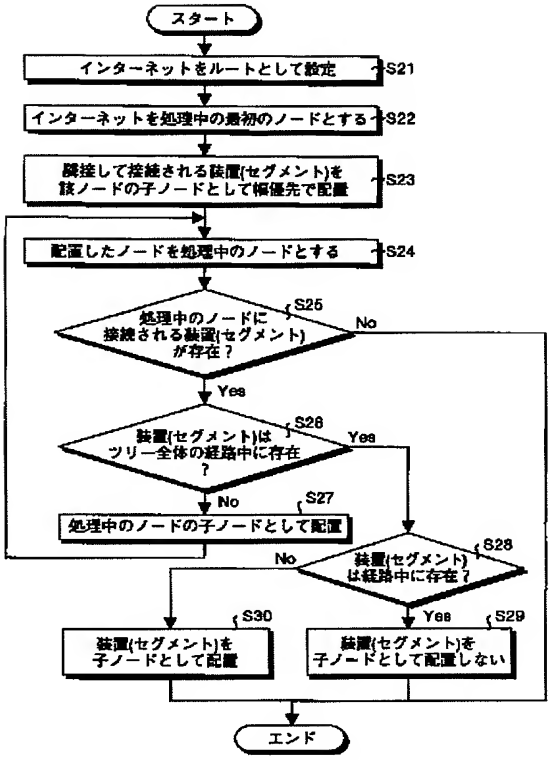
【図１４】



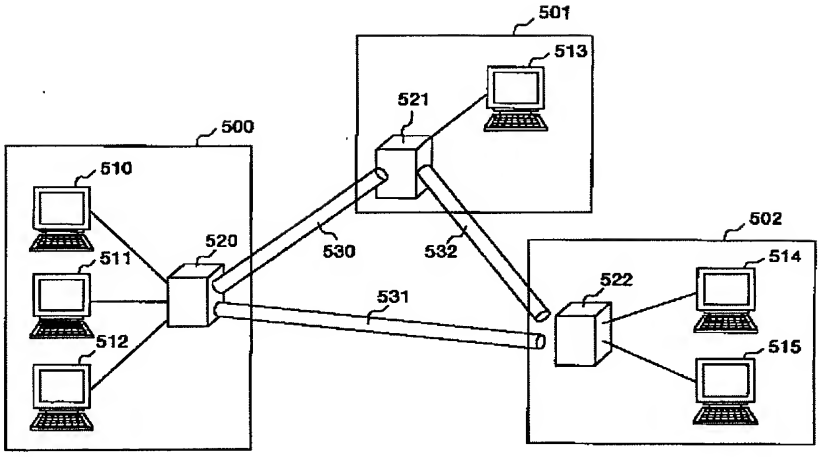
【図１５】


インターネット
411
セグメント1
403
VPN装置C
=第一VPN
セグメント2
401
サーバA
=第一エンド
経路（A）
ホストB
402
セグメント3
404
ルータJ
セグメント4
405
FW装置D
=第二外部FW
経路（B）
セグメント5
410
ホストF
407
ホストG
408
ホストH
409
406
VPN装置E
=第二VPN
セグメント5
410
407
=第二エンド
ホストG
408
ホストH
409

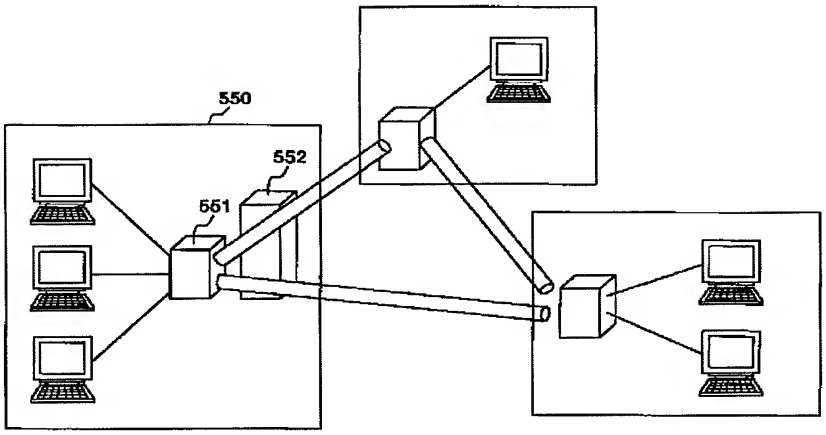
【図１６】


スタート
インターネットをルートとして設定
S21
インターネットを処理中の最初のノードとする
S22
隣接して接続される装置(セグメント)を
該ノードの子ノードとして帳優先で配置
S23
配置したノードを処理中のノードとする
S24
処理中のノードに
接続される装置(セグメント)
が存在？
S25
No
Yes
装置(セグメント)は
ツリー全体の経路中に存在
？
S26
Yes
No
S27
処理中のノードの子ノードとして配置
No
装置(セグメント)
は経路中に存在？
S28
Yes
S30
装置(セグメント)を
子ノードとして配置
S29
装置(セグメント)を
子ノードとして配置しない
エンド

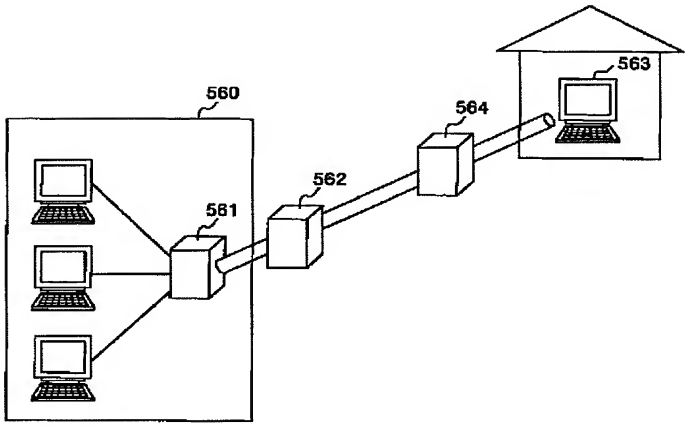
【図１７】


501
513
521
500
510
520
511
512
530
532
502
514
522
531
515

【図１８】



【図１９】



フロントページの続き

(72)発明者　高野　啓
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　金枝上　敦史
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

Ｆターム(参考)　5K030 GA15 GA17 HA08 HC01 JA10 KA07 LB05 MD04 MD06